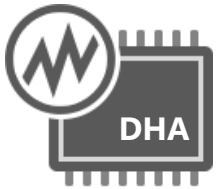


Endpoint security assurance with Device Health Attestation service (DHA)

Kam Kouladjie – Senior Program Manager, WDG
kamk@Microsoft.com

Microsoft

REDMOND
INTEROPERABILITY PLUGFEST
JUNE 19-23, 2017

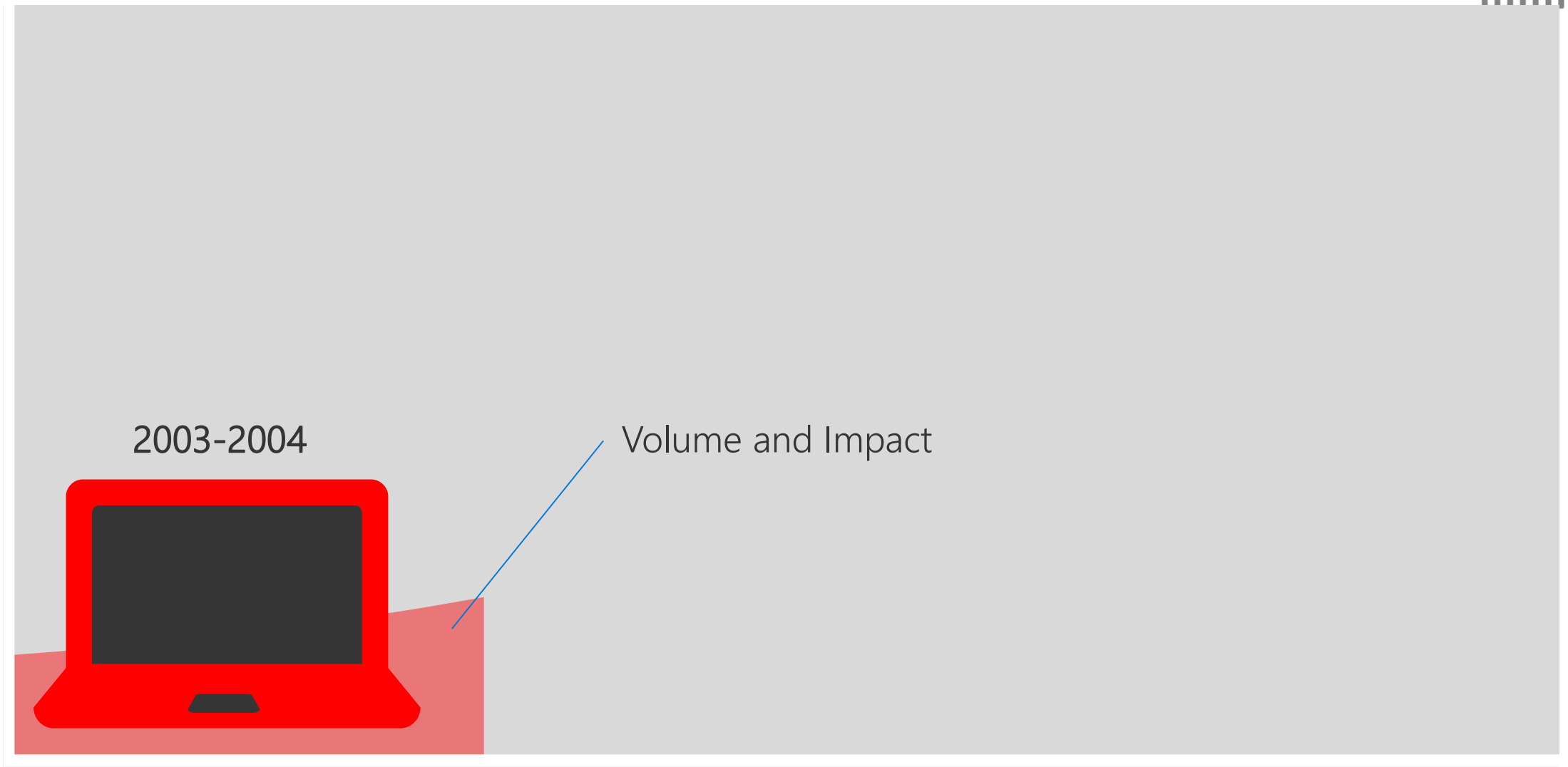
Session objectives

1. Learn more about advance threats & security challenges that impact enterprises

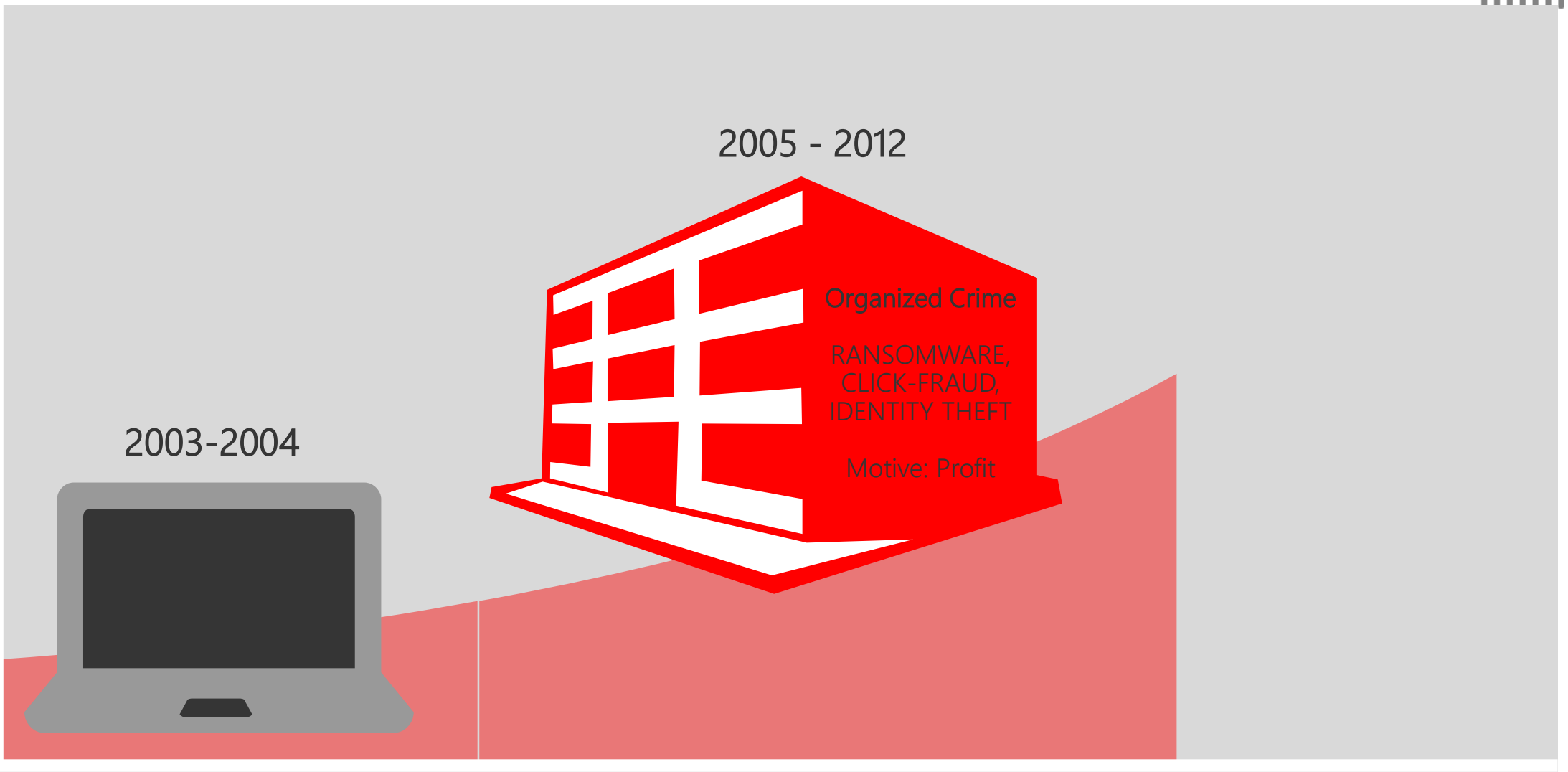
2. Learn how you can protect enterprise assets from compromised devices using Windows 10 Device Health Attestation service

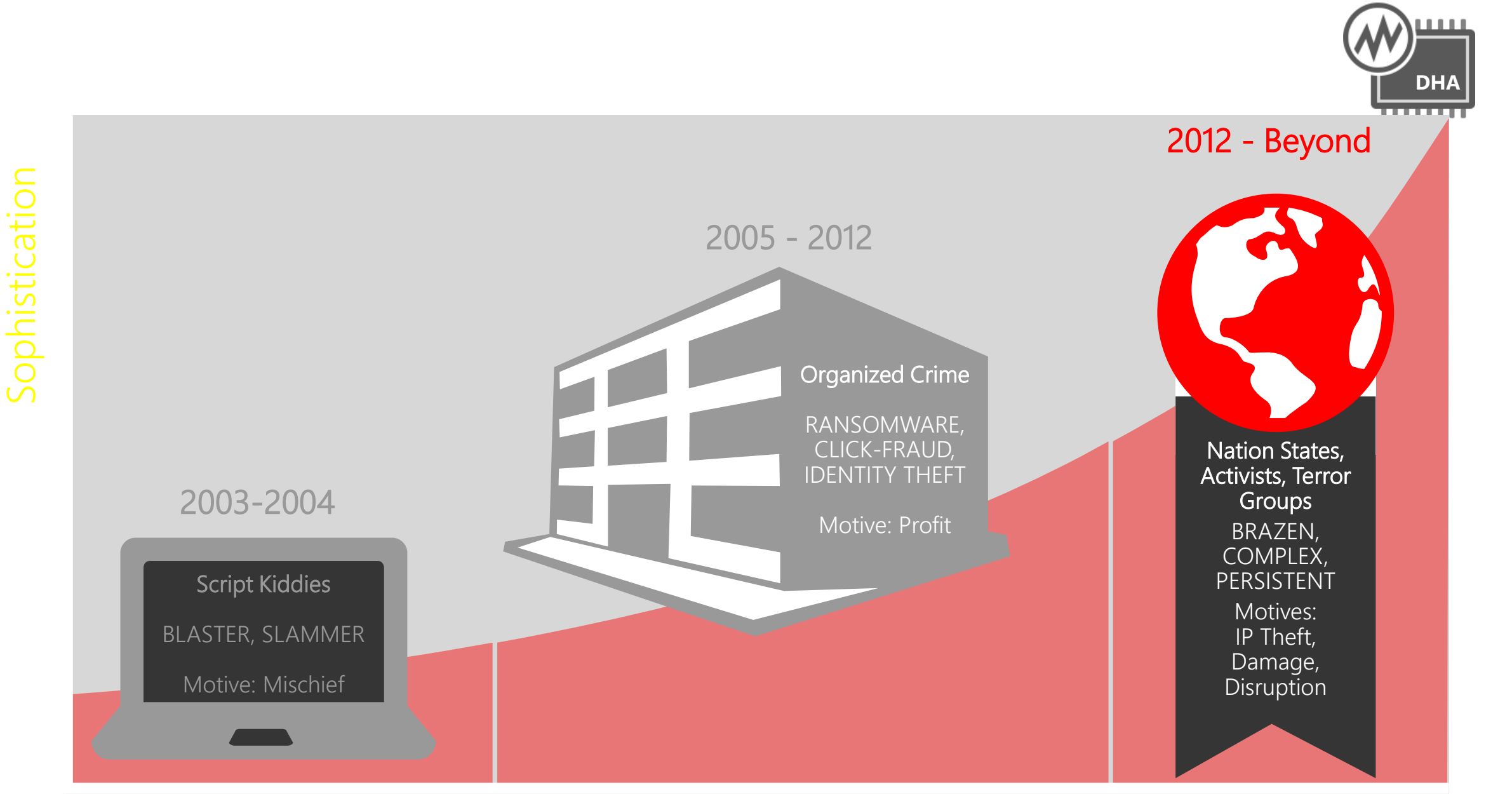
What are some of the security challenges that impact enterprises today?

The evolution of attacks



The evolution of attacks




DHA
Sophistication
2012 - Beyond
2005 - 2012
Organized Crime
RANSOMWARE,
CLICK-FRAUD,
IDENTITY THEFT
Motive: Profit
2003-2004
Script Kiddies
BLASTER, SLAMMER
Motive: Mischief
Nation States,
Activists, Terror
Groups
BRAZEN,
COMPLEX,
PERSISTENT
Motives:
IP Theft,
Damage,
Disruption

Targeting

A SANS Survey

Written by Barbara Filkins

Advisor: G. Mark Hardy

February 2016

Top Spending Areas for Skills and Technology

Skill

Spending Area	% Respondents
Application security	76%
Compliance	76%
Data security	74%

Technology

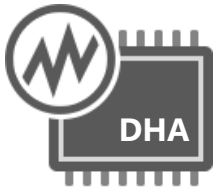
Spending Area	% Respondents
Access and authentication	88%
Advanced malware protection	80%
Endpoint protection	75%

Top Business Drivers for Security Spending

Protection of sensitive data

Regulatory compliance

Reducing incidents and breaches



Enterprises are increasingly exposed to a new class of exploits that:

Infect a device at runtime, or via supply chain attack surfaces

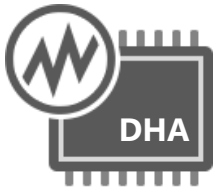
Exploit firmware bugs, early boot component code and device boot configuration vulnerabilities

Hide themselves from Windows security stack, capable of remaining obfuscated from local or remote detection

Persist across multiple boots or recovery sessions

Survive clean installations and re-imaging

Used to compromise enterprises' valuable assets directly, or abused as a launch pad for multi-phased attacks or a backdoor for future exploits



Microsoft Security Bulletin MS15-111 - Important

62 out of 103 rated this helpful - Rate this topic

Security Update for Windows Kernel to Address Elevation of Privilege (3096447)

Published: October 13, 2015 | Updated: October 16, 2015

Version: 1.1

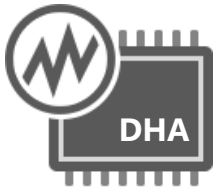
Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.

Note Customers who are using local and remote reporting attestation solutions should review the details of CVE-2015-2552 discussed in this bulletin.

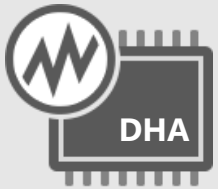
Can I detect Secure Boot tampering in my enterprise environment?

Enterprises that use the Windows 10 Device Health Attestation feature can detect this jailbreak technique. **Please contact your Device Management Solution Provider for more information about how you can use Windows 10 Device Health Attestation feature to address the identified risk.**



Questions?

Identifying the weakest link…



Manufacturing

TPM Manufacturer

OEM

Supply chain

Shipping

Datacenter

Provisioning

Daily operation

Back-up (archival)

Business continuity & disaster recovery

Decommission

Breach *(Unauthorized access)*

- Malicious actor (external)
- Malicious admin
- Malicious operator
- Logic bombs, zombies, automated attacks,..

Error

- Admin
- Operator

Bugs

- Firmware
- Boot component
- Kernel/system level
- Application – Win 32/64
- Application – UAP

Config. issues

- Boot *(CI policy, SBCP policy, test signing,..)*
- Runtime policies

Attestation

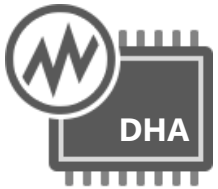
- Host (Windows, *nix)
- Clients (Windows, *nix, IOS,..)

Continuous diagnostics

Offline detection (log monitoring)

Automated retention

Automated audit



Introduction to TPM

(Trusted Platform Module)

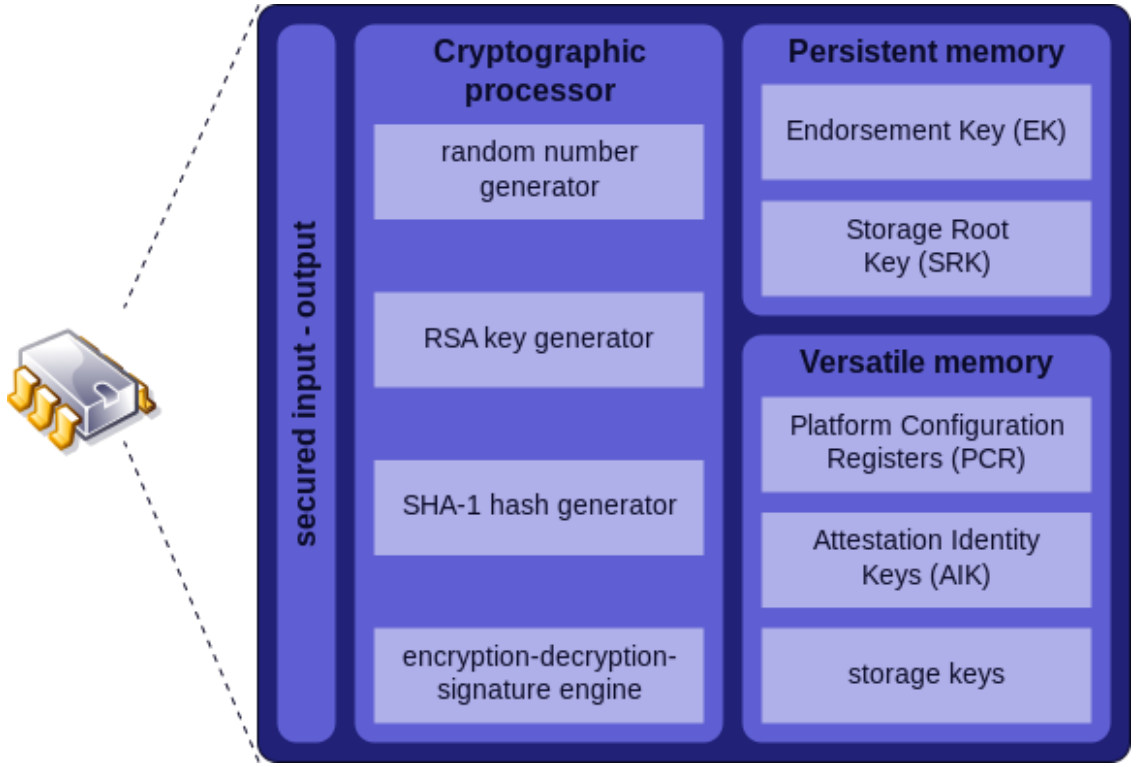
TPM Types

Discrete TPM *(Laptop, Desktop, Servers)*

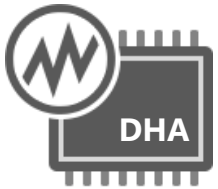
Virtual TPM *(Virtual PC)*

Firmware TPM *(Phone, Tablet, Laptop,..)*

TPM components

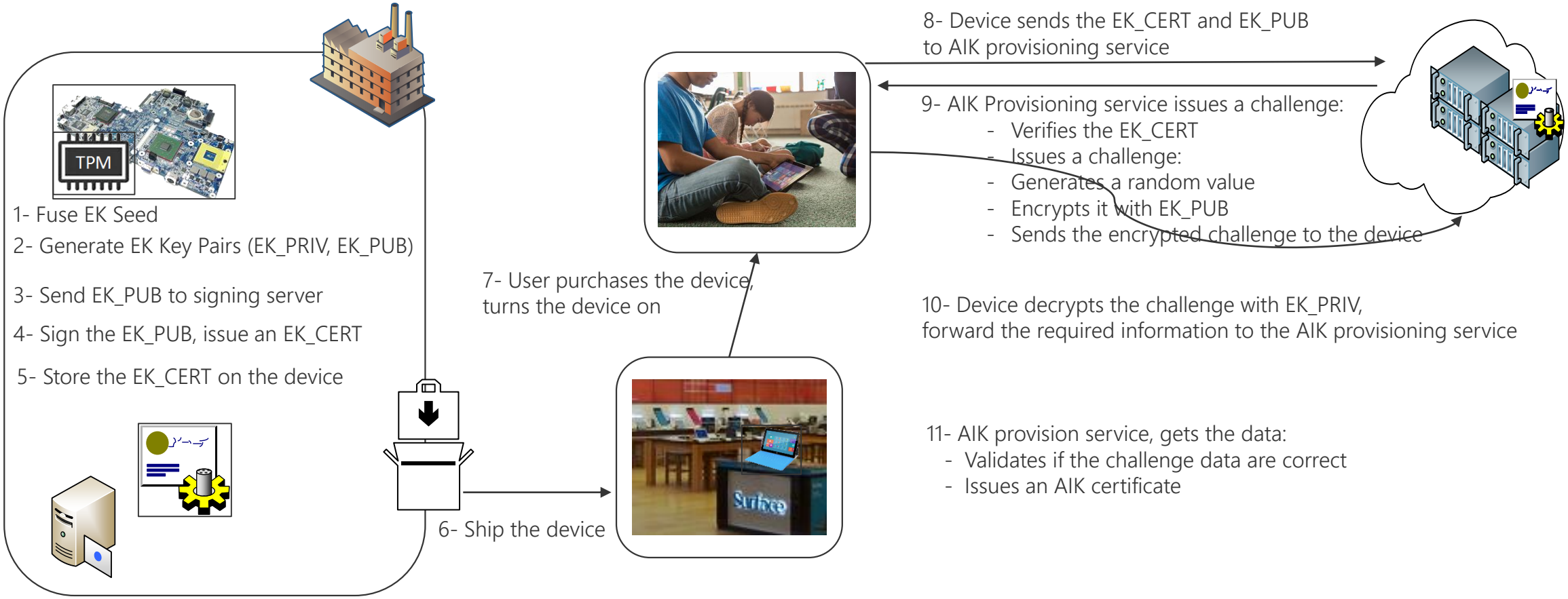


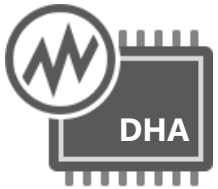
TPM certificates



- **EK certificate**
  - EK public key signed in OEM factory
  - Used to enable remote attestation of the device
- **AIK certificate**
  - AIK public key signed by Microsoft after remote attestation of the device to the AIK provisioning service
  - Designed to reduce privacy risks

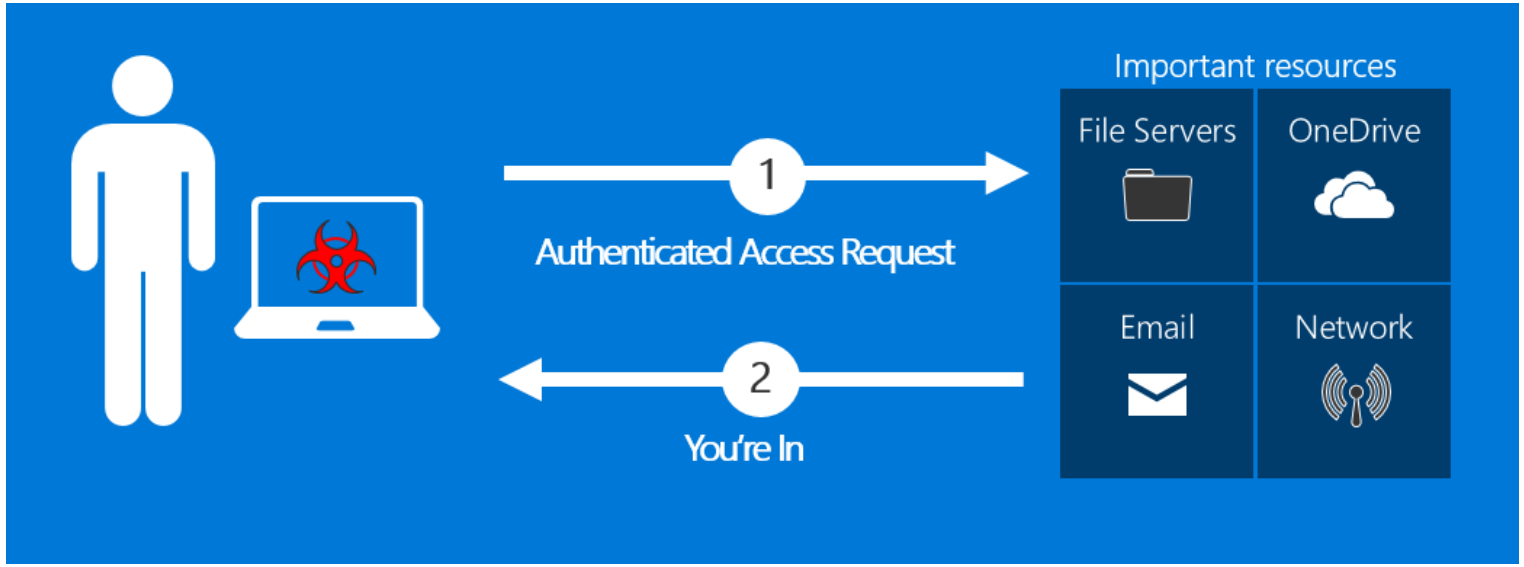
TPM secrets, certificates & manufacturing *(sample flow)*

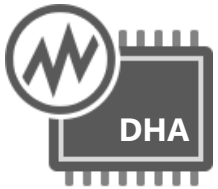




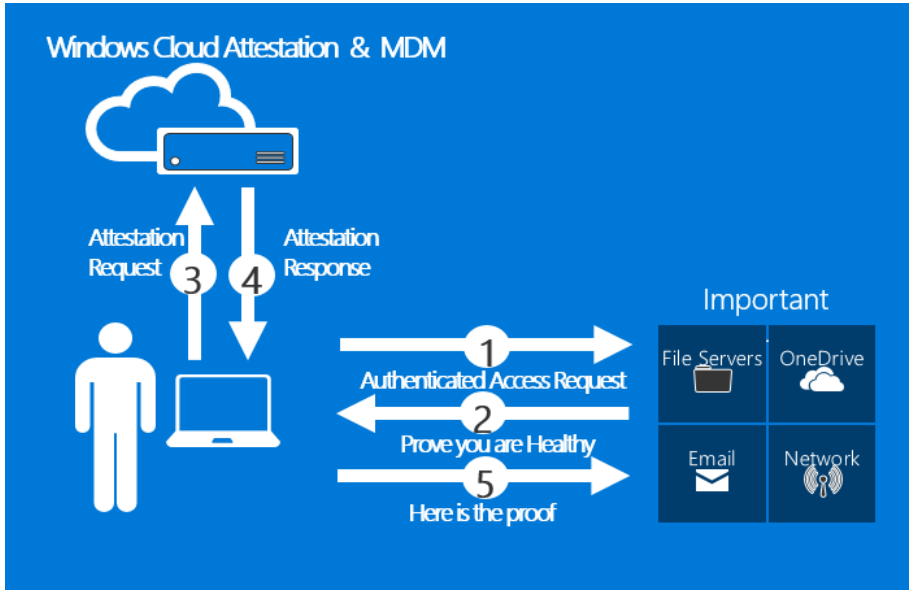
What is Device Health Attestation (DHA) ?

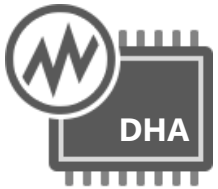
Before Windows 10 Device Health Attestation (DHA) release device health was assumed





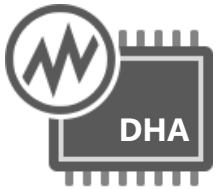
Device Health Attestation (DHA) enables enterprises to validate device health remotely based on hardware measured & attested data





Device Health Attestation builds upon existing Windows security technologies that were released in Windows 8

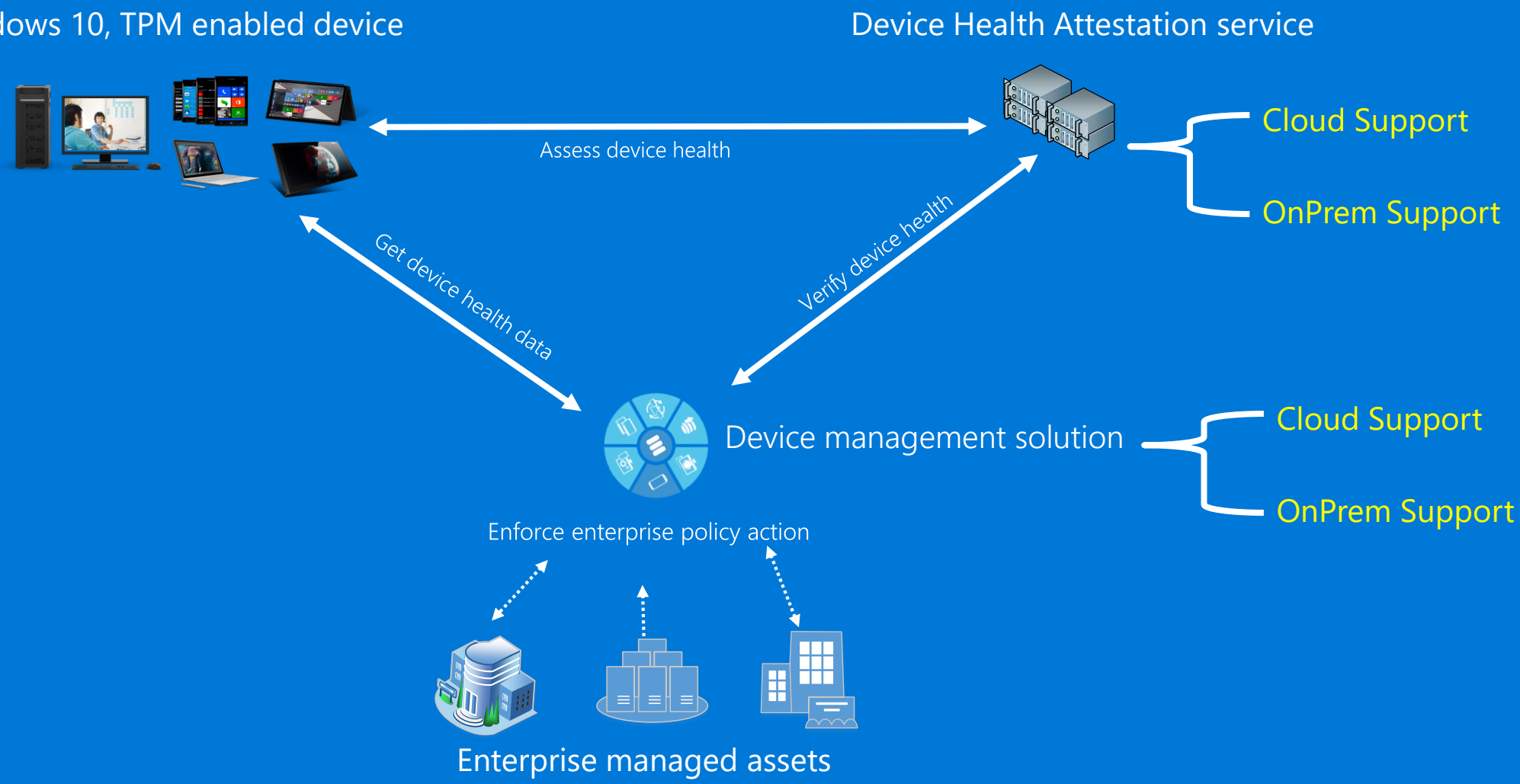
- Secure Boot
- Measured Boot
- Early Launch Anti-Malware
- TPM Attestation



DHA enables IT administrators to monitor device health remotely based on "**TPM protected**", "**tamper resistant**" and "**tamper evident**" data.

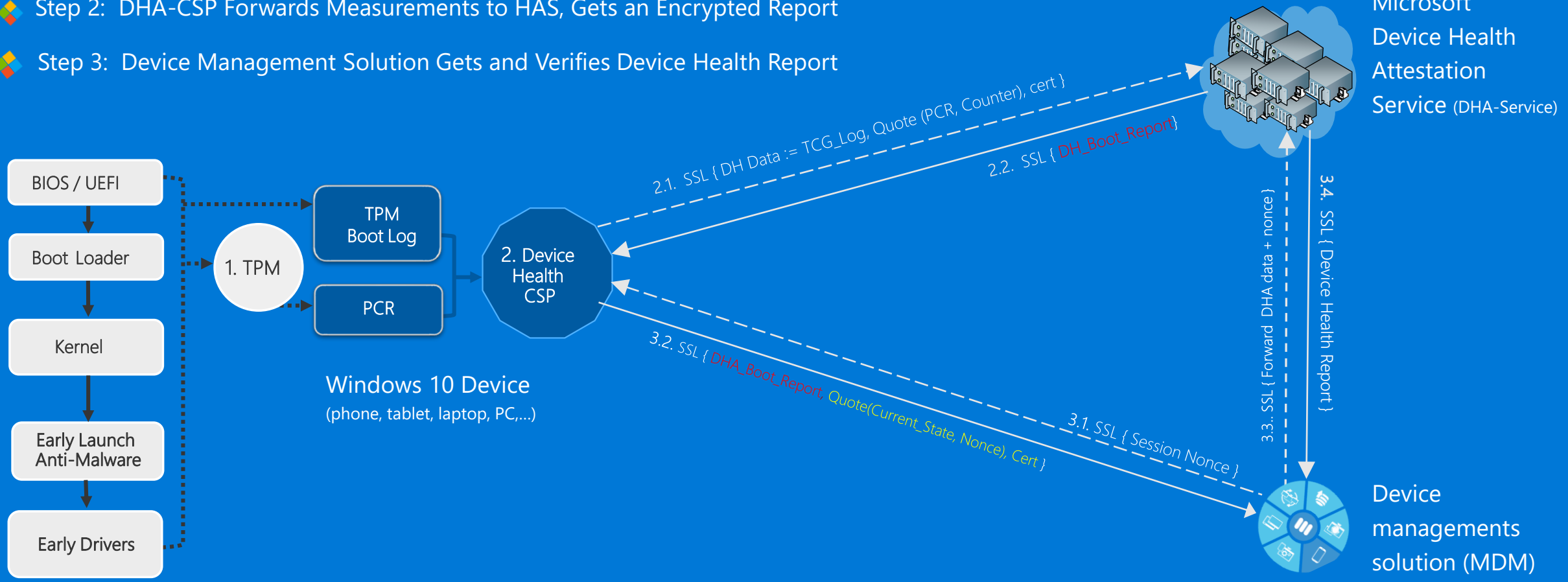
DHA Components

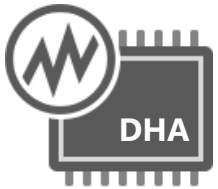
Microsoft Windows 10 DHA



Microsoft
Windows 10 DHA

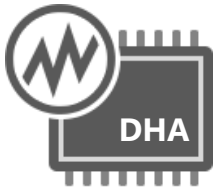
- Step 1: Device Measures Boot Components in the TPM
- Step 2: DHA-CSP Forwards Measurements to HAS, Gets an Encrypted Report
- Step 3: Device Management Solution Gets and Verifies Device Health Report



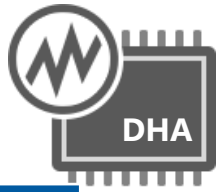


Sample data points that are evaluated/reported by DHA-Service

- BitlockerStatus
- SecureBootEnabled
- CodeIntegrityEnabled
- ELAMDriverLoaded
- VSMEnabled
- CIPolicyHash
- SBCPPolicyHash
- DEPPolicy State
- SafeMode
- WinPE
- BootDebuggingEanabled
- OSKernelDebuggingEnabled
- TestSigningEnabled
- AIKCertPresent
- Value of PCR 0
- Reset Count (Hibernation)
- Restart Count (Boot/reboot)
- And more ….

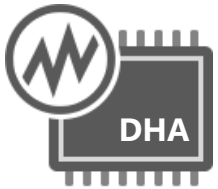


Implementation Options?



DHA - Implementation options

DHA-Cloud	Microsoft owned and operated service running in 4 datacenter *<free>*
DHA-OnPrem	DHA-Services running on Server 2016 *<no added/extra licensing fee>*
DHA-Azure	DHA-Services running on Server 2016 *<Azure traffic/usage cost>*



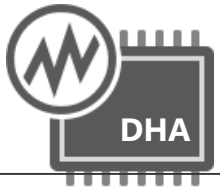
List of DHA-Enabled capabilities

- Data Collection (*i.e. Anomaly analysis, Audit*)
- Compliance Reporting *(i.e. On demand, Scheduled)*
- Live Monitoring *(i.e. Continuous diagnostics)*
- Zero Day Incident Response *(i.e. Incident Response Agility)*
- Online Enforcement *(i.e. Conditional Access)*
- Out of band enforcement *(i.e. Alert, notification, expiring access tokens..)*

*** Please contact your MDM for a full/more up-to-date list.. ***

DHA-Enabled MDM's

DHA dependencies



Endpoint Software:

- Windows 10 RTM (All editions)
- Windows 10 Mobile
- Windows Server 2016

Endpoint Hardware:

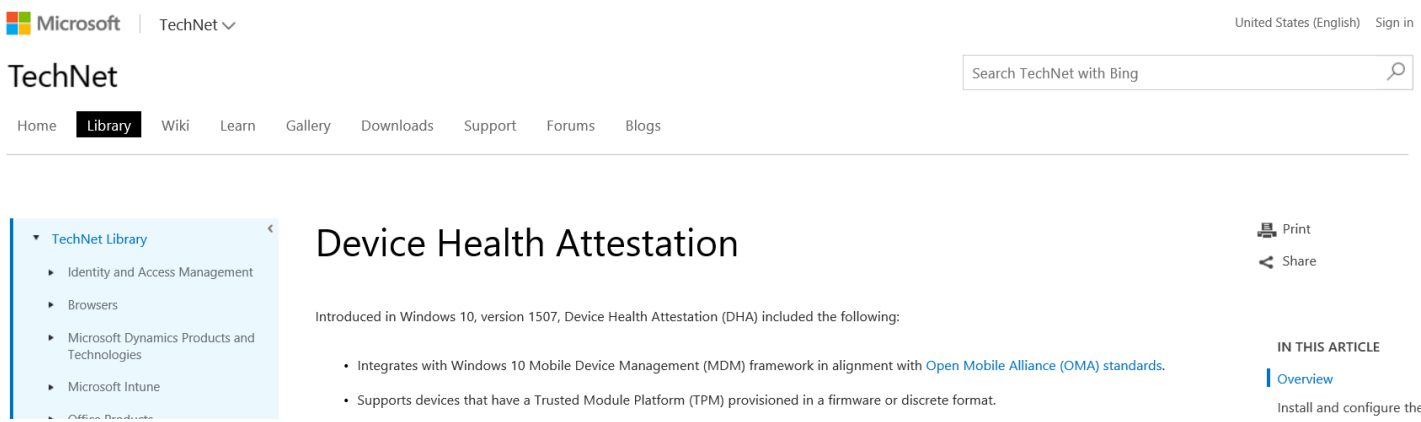
- TPM is required
- Win 10 RTM & TH2 (build 10586):
  - TPM 2.0 Required
- Windows Redstone:
  - TPM 1.2 support will be added

Attestation Server/Service:

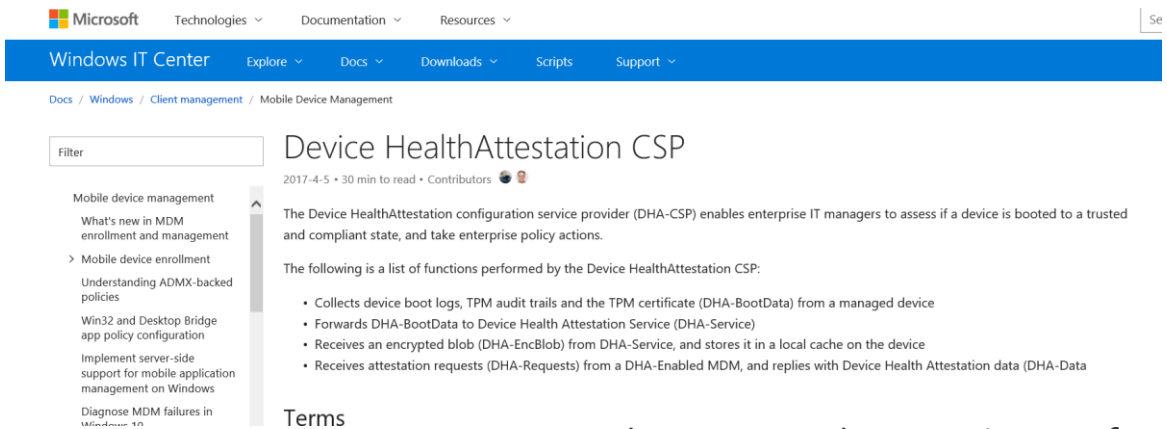
- Cloud Service:
  - Microsoft Heath Attestation Service
- On Premise Server:
  - Windows Server 2016 Health Attestation Server Role

Device Management Solution :

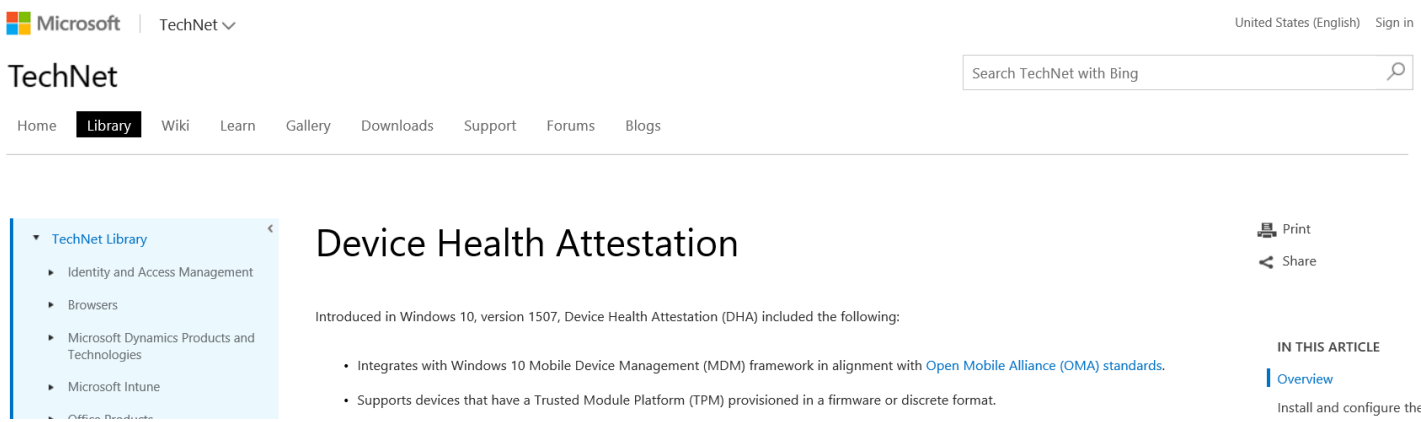
- Microsoft Intune
- System Center Config Manager (SCCM)
- Airwatch
- MobileIron
- SOTI
- Citrix
- Symantec,
- More .....



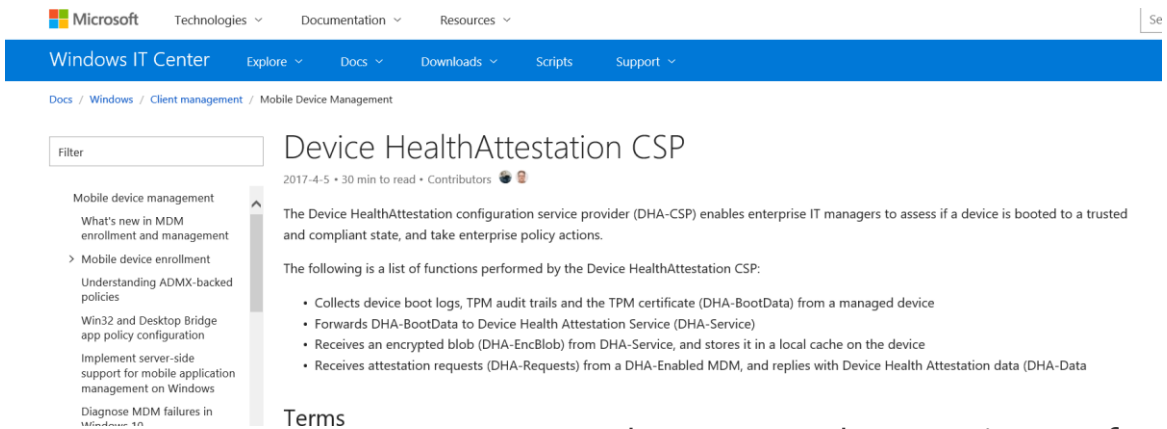
https://technet.microsoft.com/en-us/library/mt750346.aspx



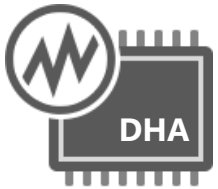
https://technet.microsoft.com/en-us/library/mt750346.aspx



https://technet.microsoft.com/en-us/library/mt750346.aspx

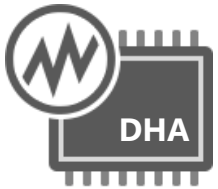


https://technet.microsoft.com/en-us/library/mt750346.aspx



More questions?

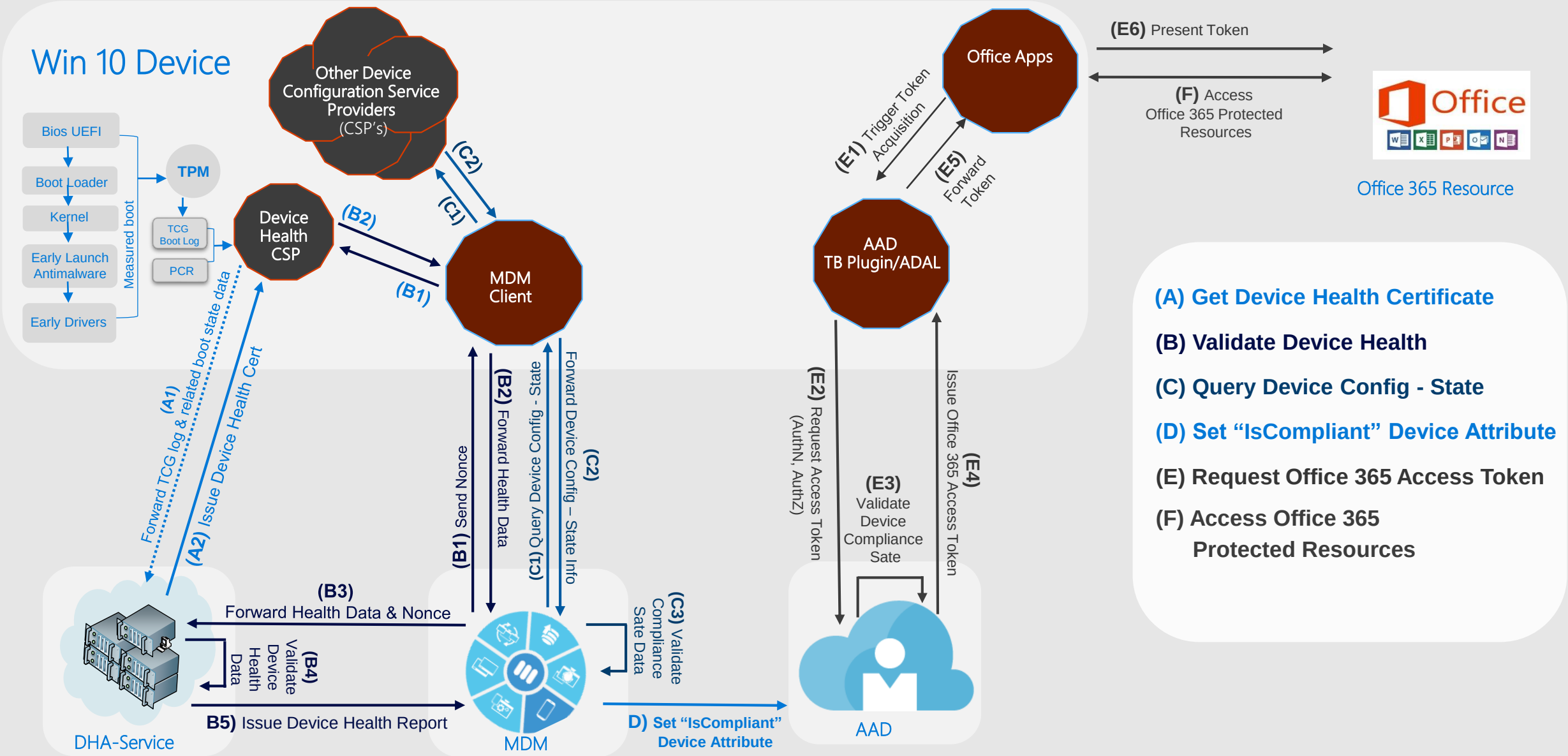
kamk@Microsoft.com



Thank you!

DHA-Enabled MDM – O365 CA flow

Microsoft Windows 10 DHA



(A) Get Device Health Certificate

(B) Validate Device Health

(C) Query Device Config - State

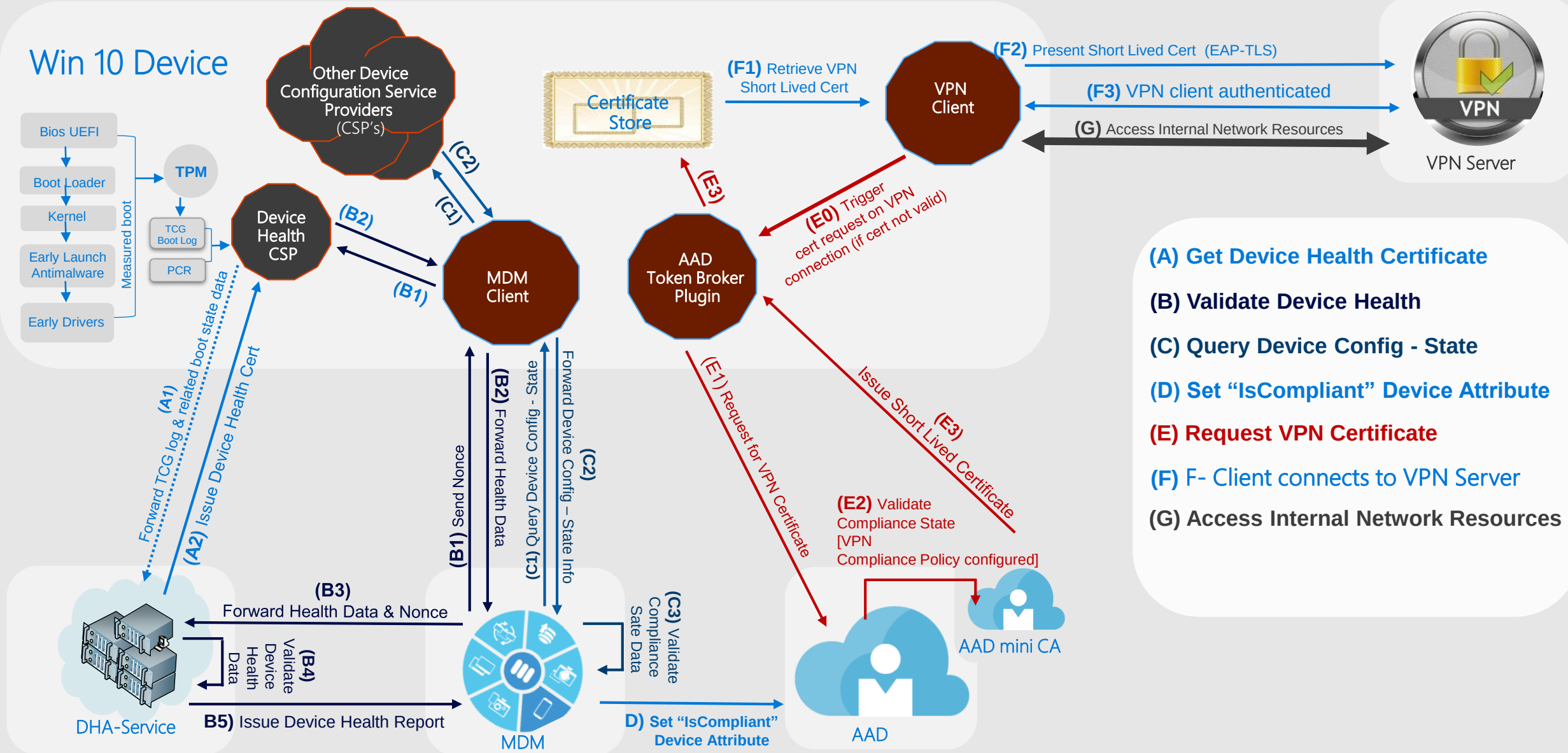
(D) Set "IsCompliant" Device Attribute

(E) Request Office 365 Access Token

(F) Access Office 365 Protected Resources

DHA-Enabled MDM – VPN CA flow

Microsoft Windows 10 DHA



(A) Get Device Health Certificate

(B) Validate Device Health

(C) Query Device Config - State

(D) Set "IsCompliant" Device Attribute

(E) Request VPN Certificate

(F) F- Client connects to VPN Server

(G) Access Internal Network Resources